


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)
**Search:** ☒ The ACM Digital Library ☐ The Guide



 Searching within **The ACM Digital Library** for: bootup virtualization (start a new search)

Found 11 of 245,263

**REFINE YOUR SEARCH**

## ▼ Refine by Keywords

Discovered Terms

## ▼ Refine by People

 Names  
Institutions  
Authors

## ▼ Refine by Publications

 Publication Year  
Publication Names  
ACM Publications  
All Publications  
Content Formats  
Publishers

## ▼ Refine by Conferences

 Sponsors  
Events  
Proceeding Series

**ADVANCED SEARCH**

**FEEDBACK**


Found 11 of 245,263

Search Results

Related Journals

Related SIGs

Related Conferences

Results 1 - 11 of 11

 Sort by  in 

**1** Traps, events, emulation, and enforcement: managing the yin and yang of virtualization-based security

Sergey Bratus, Michael E. Locasto, Ashwin Ramaswamy, Sean W. Smith

 October 2008 **VMSec '08**: Proceedings of the 1st ACM workshop on Virtual machine security

**Publisher:** ACM

 Full text available:  (221.17 KB) **Additional Information:** full citation, abstract, references, index terms

**Bibliometrics:** Downloads (6 Weeks): 26, Downloads (12 Months): 84, Citation Count: 0

We question current trends that attempt to leverage virtualization techniques to achieve security goals. We suggest that the security role of a virtual machine centers on being policy interpreter rather than a resource provider. These two roles (security ...

**Keywords:** debugging, security policy, traps, virtualization

**2** Devirtualizable virtual machines enabling general, single-node, online maintenance

David E. Lowell, Yasushi Saito, Eileen J. Samberg

 December 2004 **ASPLOS-XI**: Proceedings of the 11th international conference on Architectural support for programming languages and operating systems

**Publisher:** ACM

 Full text available:  (174.01 KB) **Additional Information:** full citation, abstract, references, cited by, index terms

**Bibliometrics:** Downloads (6 Weeks): 12, Downloads (12 Months): 127, Citation Count: 7

Maintenance is the dominant source of downtime at high availability sites. Unfortunately the dominant mechanism for reducing this downtime, cluster rolling upgrade, has two shortcomings that have prevented its broad acceptance. First, cluster-style ...

**Keywords:** availability, online maintenance, planned downtime, virtual machines

Also published in:

 November 2004 **SIGPLAN Notices**

Volume 39 Issue 11

 December 2004 **SIGOPS Operating Systems Review**

Volume 38 Issue 5

 December 2004 **SIGARCH Computer Architecture News**

Volume 32 Issue 5

**3** SVGrid: a secure virtual environment for untrusted grid applications

Xin Zhao, Kevin Borders, Atul Prakash

 November 2005 **MGC '05**: Proceedings of the 3rd international workshop on Middleware for grid computing

**Publisher:** ACM

 Full text available:  (409.68 KB) **Additional Information:** full citation, abstract, references, index terms

**Bibliometrics:** Downloads (6 Weeks): 6, Downloads (12 Months): 54, Citation Count: 0

Most grid security researches focus on user authentication and secure communication,

the protection of grid computers is left to the underlying operating system .  
Unfortunately, most OS level protection mechanisms can be turned off after an attacker manages ...

**Keywords:** grid computing, secure grid system, virtual machine

#### 4 [Flexible security configuration for virtual machines](#)



Sandra Ruada, Yogesh Sreenivasan, Trent Jaeger

October 2008 **CSAW '08: Proceedings of the 2nd ACM workshop on Computer security architectures**

**Publisher:** ACM

Full text available: Pdf (517.78 KB) **Additional Information:** full citation, abstract, references, index terms

**Bibliometrics:** Downloads (6 Weeks): 29, Downloads (12 Months): 92, Citation Count: 0

Virtual machines are widely accepted as a promising basis for building secure systems. However, while virtual machines offer effective mechanisms to create isolated environments, mechanisms that offer controlled interaction among VMs are immature. Some ...

**Keywords:** access control, compliance, policy, virtual machines

#### 5 [Reviews: Review of Scalent's virtual operating environment](#)

Logan G. Harbaugh

October 2008 **Linux Journal** , Volume 2008 Issue 174

**Publisher:** Specialized Systems Consultants, Inc.

Full text available: Html (12.09 KB) **Additional Information:** full citation, index terms

**Bibliometrics:** Downloads (6 Weeks): 3, Downloads (12 Months): 59, Citation Count: 0

#### 6 [FIDES: An advanced chip multiprocessor platform for secure next generation mobile terminals](#)



Hiroaki Inoue, Junji Sakai, Sunao Torii, Masato Edahiro

December 2008 **Transactions on Embedded Computing Systems (TECS)** , Volume 8 Issue 4

**Publisher:** ACM

Full text available: Pdf (2.20 MB) **Additional Information:** full citation, abstract, references, index terms

**Bibliometrics:** Downloads (6 Weeks): 34, Downloads (12 Months): 198, Citation Count: 0

We propose a secure platform on a chip multiprocessor, FIDES, in order to enable next generation mobile terminals to execute downloaded native applications for Linux. Its most important feature is the higher security based on multigrained separation ...

**Keywords:** SELinux, Secure mobile terminal, chip multiprocessor

#### 7 [Dynamic and adaptive updates of non-quiescent subsystems in commodity operating system kernels](#)



Kristin Makris, Kyung Dong Ryu

June 2007 **EuroSys '07: Proceedings of the 2nd ACM SIGOPS/EuroSys European Conference on Computer Systems 2007**

**Publisher:** ACM

Full text available: Pdf (452.03 KB) **Additional Information:** full citation, abstract, references, index terms

**Bibliometrics:** Downloads (6 Weeks): 8, Downloads (12 Months): 92, Citation Count: 2

Continuously running systems require kernel software updates applied to them without downtime. Facilitating fast reboots, or delaying an update may not be a suitable solution.

in many environments, especially in pay-per-use high-performance computing ...

**Keywords:** DynAMOS, adaptive operating system, dynamic instrumentation, dynamic software updates, function cloning

Also published in:


June 2007 **SIGOPS Operating Systems Review** Volume 41 Issue 3

## 8 Making information flow explicit in HiStar

Nickola Zeldovich, Silas Boyd-Wickizer, Eddi Kohler, David Mazieres

November 2006 **OSDI '06: Proceedings of the 7th symposium on Operating systems design and implementation**

**Publisher:** USENIX Association

Full text available:  Pdf (293.85 KB) **Additional Information:** full citation, abstract, references

**Bibliometrics:** Downloads (6 Weeks): 6, Downloads (12 Months): 52, Citation Count: 5


HiStar is a new operating system designed to minimize the amount of code that must be trusted. HiStar provides strict information flow control, which allows users to specify precise data security policies without unduly limiting the structure of applications. ...

## 9 FIDES: an advanced chip multiprocessor platform for secure next generation mobile terminals

Hiroaki Inoue, Akihisa Ikeno, Masaki Kondo, Junji Sakai, Masato Edahiro

September 2005 **CODES+ISSS '05: Proceedings of the 3rd IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis**

**Publisher:** ACM

Full text available:  Pdf (295.94 KB) **Additional Information:** full citation, abstract, references, cited by, index terms

**Bibliometrics:** Downloads (6 Weeks): 5, Downloads (12 Months): 37, Citation Count: 4

We propose a secure platform on a chip multiprocessor, known as FIDES, in order to enable next generation mobile terminals to execute downloaded native applications for Linux. Its most important feature is the higher security based on multi-grained separation ...


**Keywords:** chip multiprocessor, linux, secure mobile terminal

## 10 Evil twins: two models for TCB reduction in HPC clusters

Jacob Gorm Hansen, Eske Christiansen, Eric Jul

July 2007 **SIGOPS Operating Systems Review**, Volume 41 Issue 4

**Publisher:** ACM

Full text available:  Pdf (1.13 MB) **Additional Information:** full citation, abstract, references, index terms

**Bibliometrics:** Downloads (6 Weeks): 7, Downloads (12 Months): 73, Citation Count: 0

Traditional high performance computing systems require extensive management and suffer from security and configuration problems. This paper presents two generations of a cluster-management system that aims at making clusters as secure and self-managing ...

## 11 Enabling scalability and performance in a large scale CMP environment

Bratin Saha, Ali-Reza Adl-Tabatabai, Anwar Ghuloum, Mohan Rajagopalan, Richard L. Hudson, Leif Petersen, Vijay Menon, Brian Murphy, Tatiana Shpeisman, Eric Sprangle, Anwar Rohillah, Doug Carmean, Jesse Fang

June 2007 **EuroSys '07: Proceedings of the 2nd ACM SIGOPS/EuroSys European Conference on Computer Systems 2007**

**Publisher:** ACM

Full text available:  Pdf (248.88 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

**Bibliometrics:** Downloads (6 Weeks): 41, Downloads (12 Months): 443, Citation Count: 3

Hardware trends suggest that large-scale CMP architectures, with tens to hundreds of processing cores on a single piece of silicon, are imminent within the next decade. While existing CMP machines have traditionally been handled in the same way as SMPs, ...

**Keywords:** memory management, multi-core processors, parallel programming, runtime design, scheduler design, sequestered mode, synchronization primitives, transactional memory

Also published in:

June 2007 **SIGOPS Operating Systems Review** Volume 41 Issue 3

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2009 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  Adobe Acrobat  QuickTime  Windows Media Player  Real Player